RECEIVED
CENTRAL FAX CENTER
JUN 17 2005

DILLON & YUDELL LLP
ATTORNEYS AT LAW

USPTO FACSIMILE TRANSMITTAL SHEET

TO: Examiner Christian A. La Forgia	FROM: Matthew W. Baca, Reg. No. 42,277
ORGANIZATION: US Patent and Trademark Office	DATE: June 17, 2005
ART UNIT: 2131 / CONFIRMATION NO.:	TOTAL NO. OF PAGES INCLUDING COVER: 18
FAX NUMBER: 703-872-9306	APPLICATION SERIAL NO: 09/696,518
ENCLOSED: Appeal Brief	ATTORNEY DOCKET NO: FR919990110US1

☒ URGENT ☐ FOR REVIEW ☐ PLEASE COMMENT ☐ PLEASE REPLY ☐ PLEASE RECYCLE

NOTES/COMMENTS:

8911 N. CAPITAL OF TEXAS HWY., SUITE 2110, AUSTIN, TEXAS 78759
512.343.6116 (V) • 512.343.6446 (F) • DILLONYUDELL.COM

RECEIVED
CENTRAL FAX CENTER
JUN 17 2005

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

ATTY. DOCKET NO.: FR919990110US1

IN RE APPLICATION OF:	§	
	§	
OLIVIER DAUDE	§	EXAMINER: **CHRISTIAN A. LA FORGIA**
	§	
SERIAL NO.: **09/696,518**	§	
	§	
FILED: **OCTOBER 25, 2000**	§	ART UNIT: **2131**
	§	
FOR: **M/S FOR PREVENTING UNAUTHORIZED SERVER INTERFERENCE IN AN INTERNET PROTOCOL NETWORK**	§	

APPEAL BRIEF UNDER 37 C.F.R. 1.192

Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

This Appeal Brief is submitted in support of an Appeal of the Examiner's final rejection of claims 1, 4, 6-10, 14, 17, 19-23, 27, 30, and 32-36. A Notice of Appeal in this case was filed and received by the patent office on April 19, 2005. Please charge the fee of $500.00 due under 37 C.F.R. § 1.17(c), as well as any additional required fees, to IBM Deposit Account No. 09-0457.

Certificate of Transmission/Mailing

I hereby certify that this correspondence is being facsimile transmitted to the USPTO at 703-872-9306 or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450 on the date shown below.

Typed or Printed Name: Michelle Sanderson *Date: June 17, 2005* *Signature:* MSanderson

06/20/2005 GWORDOF1 00000023 090457 09696518

01 FC:1402 500.00 DA

REAL PARTY IN INTEREST

The real party in interest in the present Application is International Business Machines Corporation, the Assignee of the present application as evidenced by the Assignment set forth at reel 011285, frame 0030 et. seq. of the USPTO assignment records.

RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to Appellant, the Appellant's legal representative, or assignee, which directly affect or would be directly affected by or have a bearing on the Board's decision in the pending appeal.

STATUS OF CLAIMS

Claims 1, 4, 6-10, 14, 17, 19-23, 27, 30, and 32-36 stand finally rejected by the Examiner, as noted in the Final Office Action dated January 19, 2005. The rejection of Claims 1, 4, 6-10, 14, 17, 19-23, 27, 30, and 32-36 is appealed.

STATUS OF AMENDMENTS

Appellant's Amendment A filed on July 7, 2004 was entered by the Examiner as indicated in the Final Office Action. No amendment to the claims was proposed or entered subsequent to the Final Rejection dated January 19, 2005.

SUMMARY OF THE CLAIMED SUBJECT MATTER

Appellant's invention may be implemented as a method, a system, or a computer program product operable in a dynamic host configuration protocol (DHCP) network that prevents unauthorized dynamic host configuration servers from responding to client configuration requests. The invention uses a designated server checker client that broadcasts configuration requests to draw configuration server responses which are then analyzed to detect unauthorized servers. Detected unauthorized servers are individually targeted by the server checker client with configuration requests to prevent the unauthorized servers from interacting with the network clients.

Appellant's Claim 1 provides a method for "preventing unauthorized dynamic host configuration servers from responding to client configuration requests in an Internet Protocol (IP) network," including the following steps: (1) broadcasting host configuration requests from a server checker client (*see specification* page 18, lines 14-15 and 27-28, describing with reference to FIG. 1 a DHCP client broadcasting a host configuration request, the first part of which is a DHCPDISCOVER message; page 21, lines 14-17, with reference to FIG. 2, describing a server detector component 207 sending requests (via broadcast as described with reference to FIG. 1) to retrieve configuration information); (2) receiving configuration offer messages from one or more dynamic host configuration servers, said configuration offer messages delivered to the server checker client responsive to the broadcast host configuration requests (page 19, lines 1-11, referring to FIG. 1, describing receipt by DHCP client 101 of configuration offer messages in response to the DHCPDISCOVER messages; page 21, lines 14-22, referring to FIG. 2, describing receipt of DHCOFFER messages returned by DHCP servers 203 and 204 responsive to configuration requests sent by checker client 205); (3) detecting an unauthorized dynamic host configuration server within said IP network in accordance with server identification data within the configuration offer messages (page 21, lines 17-22, referring to FIG. 2, describing invalid server detector 207 detecting one or more unauthorized servers within IP network 202 by comparing a "server identifier" option in the configuration offer messages with authorized server identification data in a DHCP server table 206); and (4) responsive to said detecting step, unicasting host configuration requests from said server checker client to said unauthorized dynamic configuration server such that said unauthorized dynamic host configuration server is unable to respond to configuration requests from network clients (page 21, line 24 through page 22, line 3, referring to FIG. 2, describing an invalid server denial handler component 208 sending multiple requests (including DHCPDISCOVER messages and the second part of an overall host configuration request called a DHCPREQUEST – see page 19, lines 11-17) directed to each detected unauthorized server 204).

The invention recited in Claim 14 provides a system for preventing unauthorized dynamic host configuration servers from responding to client configuration requests in an IP network. The system includes: (1) processing means for broadcasting host configuration requests from a server checker client (*see specification* page 18, lines 14-15 and 27-28, describing with reference to FIG. 1 a DHCP client broadcasting a host configuration request, the

first part of which is a DHCPDISCOVER message; page 21, lines 14-17, with reference to FIG. 2, describing a server detector component 207 sending requests (via broadcast as described with reference to FIG. 1) to retrieve configuration information); (2) processing means for receiving configuration offer messages from one or more dynamic host configuration servers, said configuration offer messages delivered to the server checker client responsive to the broadcast host configuration requests (page 19, lines 1-11, referring to FIG. 1, describing receipt by DHCP client 101 of configuration offer messages in response to the DHCPDISCOVER messages; page 21, lines 14-22, referring to FIG. 2, describing receipt of DHCOFFER messages returned by DHCP servers 203 and 204 responsive to configuration requests sent by checker client 205); (3) processing means for detecting an unauthorized dynamic host configuration server within said IP network in accordance with server identification data within the configuration offer messages (page 21, lines 17-22, referring to FIG. 2, describing invalid server detector 207 detecting one or more unauthorized servers within IP network 202 by comparing a "server identifier" option in the configuration offer messages with authorized server identification data in a DHCP server table 206); and (4) processing means, responsive to detecting an unauthorized dynamic host configuration server, for unicasting host configuration requests from said server checker client to said unauthorized dynamic configuration server such that said unauthorized dynamic host configuration server is unable to respond to configuration requests from network clients (page 21, line 24 through page 22, line 3, referring to FIG. 2, describing an invalid server denial handler component 208 sending multiple requests (including DHCPDISCOVER messages and the second part of an overall host configuration request called a DHCPREQUEST – see page 19, lines 11-17) directed to each detected unauthorized server 204).

The invention recited in Claim 15 provides a computer program product for preventing unauthorized dynamic host configuration servers from responding to client configuration requests in an IP network (page 20, lines 29-31, describing implementation of checker client functionality as a computer program; page 23, lines 7-9, describing a detector 207 within a checker client 205 used to detect unauthorized dynamic host configuration servers). The program product includes instruction means for: (1) broadcasting host configuration requests from a server checker client (*see* specification page 18, lines 14-15 and 27-28, describing with reference to FIG. 1 a DHCP client broadcasting a host configuration request, the first part of which is a DHCPDISCOVER message; page 21, lines 14-17, with reference to FIG. 2,

describing a server detector component 207 sending requests (via broadcast as described with reference to FIG. 1) to retrieve configuration information); (2) receiving configuration offer messages from one or more dynamic host configuration servers, said configuration offer messages delivered to the server checker client responsive to the broadcast host configuration requests (page 19, lines 1-11, referring to FIG. 1, describing receipt by DHCP client 101 of configuration offer messages in response to the DHCPDISCOVER messages; page 21, lines 14-22, referring to FIG. 2, describing receipt of DHCOFFER messages returned by DHCP servers 203 and 204 responsive to configuration requests sent by checker client 205); (3) detecting an unauthorized dynamic host configuration server within said IP network in accordance with server identification data within the configuration offer messages (page 21, lines 17-22, referring to FIG. 2, describing invalid server detector 207 detecting one or more unauthorized servers within IP network 202 by comparing a "server identifier" option in the configuration offer messages with authorized server identification data in a DHCP server table 206); and (4) responsive to said detecting step, unicasting host configuration requests from said server checker client to said unauthorized dynamic configuration server such that said unauthorized dynamic host configuration server is unable to respond to configuration requests from network clients (page 21, line 24 through page 22, line 3, referring to FIG. 2, describing an invalid server denial handler component 208 sending multiple requests (including DHCPDISCOVER messages and the second part of an overall host configuration request called a DHCPREQUEST – see page 19, lines 11-17) directed to each detected unauthorized server 204).

Appellant's Claims 8, 21, and 34 include additional features that further characterize the foregoing "detecting" step (3) by reciting "wherein said checker client includes a server table having a list of authorized dynamic host configuration servers, and wherein said step of detecting an unauthorized dynamic host configuration server further comprises comparing a server identifier included in each configuration offer message with authorized server identification data in the server table" (page 21, lines 5-12 and 17-22, referring to FIG. 2, describing DHCP Server table 206 having a list of authorized DHCP servers identified by their IP addresses).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. The Examiner's rejection of Claims 1, 8, 14, 21, 27, and 34 under 35 U.S.C. §103(a) as being unpatentable over U.S. Pat. No. 6,424,654, issued to Daizo (*Daizo* hereinafter), in view of "Authentication of DHCP Messages" issued to Droms et al. (*Droms* hereinafter), and in further view of U.S. Pat. No. 5,884,024, issued to Lim et al. (*Lim* hereinafter) is to be reviewed on Appeal; and

B. The Examiner's rejection of Claims 4, 6-7, 9-10, 17, 19-20, 22-23, 30, and 32-33, 35-36 under 35 U.S.C. §103(a) as being unpatentable over *Daizo*, in view of *Droms*, and in further view of *Lim* is to be reviewed on Appeal.

ARGUMENT

A. The rejection of Claims 1, 8, 14, 21, 27, and 34 under 35 U.S.C. §103(a) as being unpatentable over *Daizo*, *Droms*, and *Lim* is not well founded and should be reversed.

i. Claims 1, 14, and 27

1. The combination of *Daizo*, *Droms*, and *Lim* does not disclose each claimed feature of Claims 1, 14, and 27

The third element of each of Claims 1, 14, and 27 (represented in the following discussion by Claim 1) recites "detecting an unauthorized dynamic host configuration server within said IP network in accordance with server identification data within the configuration offer messages" (emphasis added). Paragraph 10, page 3 of the Final Office Action asserts, "Droms discloses detecting an unauthorized dynamic host configuration server within said IP network in accordance with server identification data within the configuration offer messages. (p. 3 - p. 4 'Section 3. Protocol 0' and 'Section 4. Protocol 1')." As argued by Appellants in the Response to the Final Office Action, while *Droms* does disclose a method for authenticating DHCP messages and entities, neither the "Protocol 0" nor "Protocol 1" method described by *Droms* at page 3, *et seq.*, authenticate the server using server identification data.

Droms's "Protocol 0" depicted in section 3, pg. 3- pg. 4, utilizes an authentication token that is known (i.e. pre-specified) to both the client and server that provides mutual

authentication. The token does not contain data relating to the identity of either the client or server.

Droms's "Protocol 1" authentication protocol uses an encrypted message authentication code and not server identification data to authenticate the server. At paragraph 4, page 4 *Droms* explains, "... the client requests authentication in its DHCPDISCOVER message and the server replies with a DHCPOFFER message that includes authentication information. This authentication information contains an encrypted value generated by the source as a message authentication code (MAC) to provide message authentication and entity authentication." (Emphasis added).

The cooperative (two-sided) aspect of *Droms's* "Protocol 1" authentication is explained at page 5: "...Protocol 1 requires a shared secret key for each client on each DHCP server with which that client may wish to use the DHCP protocol." Nothing in *Droms* suggests that the identity of the server (i.e. server identification data) is used to authenticate DHCP servers. That "server identification data" as used in Appellants' Claim 1 does not encompass any and all data that may be used to *authenticate* an entity, and is instead identification data specific to the server, is self-evident from the claim language as well as the support provided in the specification (see page 23, lines 27-30; page 24 lines 9-12, IP address used as the server identification data) and was emphasized by Appellants in the Response to the Final Office Action.

By using server identification data to detect unauthorized servers, Appellant's technique, in contrast to *Droms's* authentication protocols, does not require the two-sided authentication required when using tokens or encryption, and is instead implemented, as depicted and described with reference to FIG. 2, by a specialized "checker client" that may be inserted as a specialized application into a DHCP network without the need to otherwise alter DHCP network discourse. In the Advisory Action responsive to Appellants' Response to the Final Office Action, the Examiner provided no rebuttal to Appellants' contention that *Droms* fails to disclose "detecting an unauthorized dynamic host configuration server within said IP network in accordance with server identification data within the configuration offer messages." (Emphasis added).

The fourth element of Claim 1 recites a step of, "*responsive to said detecting step,* unicasting host configuration requests *from said server checker client* to said unauthorized dynamic configuration server such that said unauthorized dynamic host configuration server is

unable to respond to configuration requests from network clients." (Emphasis added). Significant to the invention of Claim 1 is that the configuration requests are unicast in response to detecting an unauthorized server and that the source of the configuration requests unicast to the detected unauthorized server is "said checker client" (i.e. the client that performs the broadcasting, receiving, and detecting steps as required by the preceding claim elements).

Both the first and final Office Actions assert that at col. 2, lines 28-34, *Lim* discloses "unicasting host configuration requests from said server checker client to said unauthorized dynamic configuration server such that said unauthorized dynamic host configuration server is unable to respond to configuration requests from network clients". Col. 2, lines 28-34 reads as follows:

> A second type of attack is known as "IP address hogging." For an attack of this type, a client system attempts to exhaust the supply of IP addresses by repeatedly obtaining IP leases from the DHCP server. Once the client system has leased all of the available IP address leases, network performance degrades as legitimate users are forced to wait for IP addresses.

While the means of the described "attack" is to deplete the supply of available IP addresses issued by the server, the attack itself is clearly client-to-client and therefore would not be launched from a "server checker client" (i.e. the DHCP client that, as expressly required by the limitations of Claim 1, performed the broadcasting, receiving, and detecting steps to detect unauthorized DHCP servers pursuant to its specialized "checker" functionality"). The characterization of the server checker client as the logical entity that performs the broadcasting, receiving, and detecting steps is a substantive and significant characterization of the "unicasting" step given that, as explained above, Appellants invention is designed to employ a logically (and possibly physically) discrete server checker client such that the legacy DHCP network components and protocols may remain unchanged. Nothing in *Lim*, *Droms*, and *Daizo*, individually or in any combination disclose "unicasting host configuration requests *from said server checker client* to said unauthorized dynamic configuration server" as "server checker client" is expressly characterized in the claims.

Given that the invention is fundamentally for detecting and disabling unauthorized servers, and with continued reference to the fourth element of Claim 1, another significant feature of the claimed invention is that the unicasting step is performed "responsive to said

detecting step." Even in combination, *Lim*, *Droms*, and *Daizo* do not disclose any technique or system whatsoever in which DHCP configuration requests are directed to a DHCP server in response to detecting that the server is unauthorized.

2. There is no motivation or suggestion in *Daizo*, *Droms*, and/or *Lim* to combine IP address "hogging" as described by *Lim* with the teachings of *Droms*

Lim discloses a method and apparatus for reducing the probability of IP address misuse *among clients* of a DHCP server. As explained by *Lim* at col. 2, lines 28-34, one such **problem** is known as "IP address hogging" in which a client attempts to exhaust the supply of IP addresses by repeatedly obtaining IP leases from a DHCP server. "IP address hogging" is described by *Lim* in this passage as an undesirable network phenomena and not a process step deliberately undertaken for any purpose whatsoever. The IP address hogging attack phenomena described by *Lim* is clearly an attack directed from a malicious client against other clients. Nothing in this passage or elsewhere in *Lim* discloses sending configuration requests, or any other type of messages, to a DHCP server in response to detecting that the DHCP server is question is unauthorized.

Appellants disagree with the assertion in reference item 13 on page 4 of the Final Office Action that the disclosure of *Droms* at page 2 provides motivation to combine the "IP address hogging" problem cited by *Lim* as a remedial feature of any kind. Similar to *Lim*, *Droms* describes IP address hogging as a problem and not a remedial feature to be used to "silence" an unauthorized DHCP server with respect to non-checker clients. Moreover, *Droms* does not supply the motivation since *Droms's* authentication protocols are implemented by "real" DHCP clients in a self-protective manner (i.e. since the authentication protocol is implemented across the network by the real clients, there is no need to expend bandwidth attempting to "silence" a non-authentic server).

Absent Appellants' disclosure and claims, there is clearly a lack of motivation or suggestion in any of the foregoing references to combine a described problem (i.e. IP address hogging) as a remedial feature in either or both *Droms* and *Daizo*.

ii. Claims 8, 21, and 34

The combination of *Daizo*, *Droms*, and *Lim* does not disclose each claimed feature of Claims 8, 21, and 34

Claim 8, representative also of Claims 21 and 34, recites "wherein said checker client includes a server table having a list of authorized dynamic host configuration servers, and wherein said step of detecting an unauthorized dynamic host configuration server further comprises comparing a server identifier included in each configuration offer message with authorized server identification data in the server table." This feature further underscores the distinction between using "server identification data" in Appellants' invention and the non-server specific authentication information used by *Droms's* authentication protocols.

Reference item 17 on page 5 of the Final Office Action asserts that the foregoing element is disclosed by *Droms* "Protocol 0" described in section 3 on pages 3 and 4. Nothing in the description of "Protocol 0" discloses any "list of authorized dynamic host configuration servers" or "comparing a server identifier included in each configuration offer message with authorized server identification data in the server table" to detect an unauthorized server.

B. The rejection of Claims 4, 6-7, 9-10, 17, 19-20, 22-23, 30, and 32-33, 35-36 under 35 U.S.C. §103(a) as being unpatentable over *Daizo*, *Droms*, and *Lim* is not well founded and should be reversed.

Claims 4, 6-7, 9-10, 17, 19-20, 22-23, 30, and 32-33, 35-36

Appellants do not concede than the present combination of *Daizo*, *Droms*, and *Lim* actually teaches or suggests any of the features of these dependent claims; however, these claims are directly or indirectly dependent on the independent claims 1, 14, and 27 which, as contended above by Appellants, have been incorrectly rejected under the references. By extension, the rejections of claims 4, 6-7, 9-10, 17, 19-20, 22-23, 30, and 32-33, 35-36 are not well founded and should be reversed.

CONCLUSION

Appellant has pointed out with specificity the manifest error in the Examiner's rejections, and the claim language that renders the invention patentable over the combinations of references. Appellant, therefore, respectfully requests that this case be remanded to the Examiner with instructions to issue a Notice of Allowance for all pending claims.

Respectfully submitted,

Matthew W. Baca
Reg. No. 42,277
DILLON & YUDELL LLP
8911 N. Capital of Texas Highway
Suite 2110
Austin, Texas 78759
512-343-6116

ATTORNEY FOR APPELLANT

APPENDIX

1. A method for preventing unauthorized dynamic host configuration servers from responding to client configuration requests in an Internet Protocol (IP) network, said method comprising the steps of:

broadcasting host configuration requests from a server checker client;

receiving configuration offer messages from one or more dynamic host configuration servers, said configuration offer messages delivered to the server checker client responsive to the broadcast host configuration requests;

detecting an unauthorized dynamic host configuration server within said IP network in accordance with server identification data within the configuration offer messages; and

responsive to said detecting step, unicasting host configuration requests from said server checker client to said unauthorized dynamic configuration server such that said unauthorized dynamic host configuration server is unable to respond to configuration requests from network clients.

2. (Cancelled)

3. (Cancelled)

4. The method of claim 1, said unicasting host configuration requests comprising unicasting a plurality of IP address renewal requests to said unauthorized dynamic host configuration server.

5. (Cancelled)

6. The method of claim 4, wherein each IP address renewal request includes:

a client medium access control (MAC) address that is not included within a range of valid MAC addresses utilized within the IP network.

7. The method of claim 4, wherein each IP address renewal request includes a client IP address that is not included within a range of valid IP addressed utilized in the IP network.

8. The method of claim 1, wherein said checker client includes a server table having a list of authorized dynamic host configuration servers, and wherein said step of detecting an unauthorized dynamic host configuration server further comprises comparing a server identifier included in each configuration offer message with authorized server identification data in the server table.

9. The method of claim 8, wherein said comparing a server identifier included in each configuration offer message with authorized server identification data in the server table further comprises the retrieving an IP address from each configuration offer message.

10. The method of claim 8, wherein said server table includes an IP address for each authorized dynamic host configuration server.

11. (Cancelled)

12. (Cancelled)

13. (Cancelled)

14. A system for preventing unauthorized dynamic host configuration servers from responding to client configuration requests in an Internet Protocol (IP) network, said system comprising:

processing means for broadcasting host configuration requests from a server checker client;

processing means for receiving configuration offer messages from one or more dynamic host configuration servers, said configuration offer messages delivered to the server checker client responsive to the broadcast host configuration requests;

processing means for detecting an unauthorized dynamic host configuration server within said IP network in accordance with server identification data within the configuration offer messages; and

processing means, responsive to detecting an unauthorized dynamic host configuration server, for unicasting host configuration requests from said server checker client to said unauthorized dynamic configuration server such that said unauthorized dynamic host configuration server is unable to respond to configuration requests from network clients.

15. (Cancelled)

16. (Cancelled)

17. The system of claim 14, said processing means for unicasting host configuration requests comprising processing means for unicasting a plurality of IP address renewal requests to said unauthorized dynamic host configuration server.

18. (Cancelled)

19. The system of claim 17, wherein each IP address renewal request includes:

a client medium access control (MAC) address that is not included within a range of valid MAC addresses utilized within the IP network.

20. The system of claim 17, wherein each IP address renewal request includes a client IP address that is not included within a range of valid IP addressed utilized in the IP network.

21. The system of claim 14, wherein said checker client includes a server table having a list of authorized dynamic host configuration servers, and wherein said processing means for detecting an unauthorized dynamic host configuration server further comprises processing means for comparing a server identifier included in each configuration offer message with authorized server identification data in the server table.

22. The system of claim 21, wherein said processing means for comparing a server identifier included in each configuration offer message with authorized server identification data in the server table further comprises processing means for retrieving an IP address from each configuration offer message.

23. The system of claim 21, wherein said server table includes an IP address for each authorized dynamic host configuration server.

24. (Cancelled)

25. (Cancelled)

26. (Cancelled)

27. A program product for preventing unauthorized dynamic host configuration servers from responding to client configuration requests in an Internet Protocol (IP) network, said program product comprising:

instruction means for broadcasting host configuration requests from a server checker client;

instruction means for processing configuration offer messages received from one or more dynamic host configuration servers, said configuration offer messages delivered to the server checker client responsive to the broadcast host configuration requests;

instruction means for detecting an unauthorized dynamic host configuration server within said IP network in accordance with server identification data within the configuration offer messages; and

instruction means, responsive to said detecting, for unicasting host configuration requests from said server checker client to said unauthorized dynamic configuration server such that said unauthorized dynamic host configuration server is unable to respond to configuration requests from network clients.

28. (Cancelled)

29. (Cancelled)

30. The program product of claim 27, said instruction means for unicasting host configuration requests comprising instruction means for unicasting a plurality of IP address renewal requests.

31. (Cancelled)

32. The program product of claim 30, wherein each IP address renewal request includes:

a client medium access control (MAC) address that is not included within a range of valid MAC addresses utilized within the IP network.

33. The program product of claim 30, wherein each IP address renewal request includes a client IP address that is not included within a range of valid IP addressed utilized in the IP network.

34. The program product of claim 27, wherein said checker client includes a server table having a list of authorized dynamic host configuration servers, and wherein said instruction means for detecting an unauthorized dynamic host configuration server further comprises:

instruction means for comparing a server identifier included in each configuration offer message with authorized server identification data in the server table.

35. The program product of claim 34, wherein said instruction means for comparing a server identifier included in each configuration offer message with authorized server identification data in the server table further comprises instruction means for retrieving an IP address from each configuration offer message.

36. The program product of claim 34, wherein said server table includes an IP address for each authorized dynamic host configuration server.

37. (Cancelled)

38. (Cancelled)

39. (Cancelled)